. 4.

nikto

-03-22

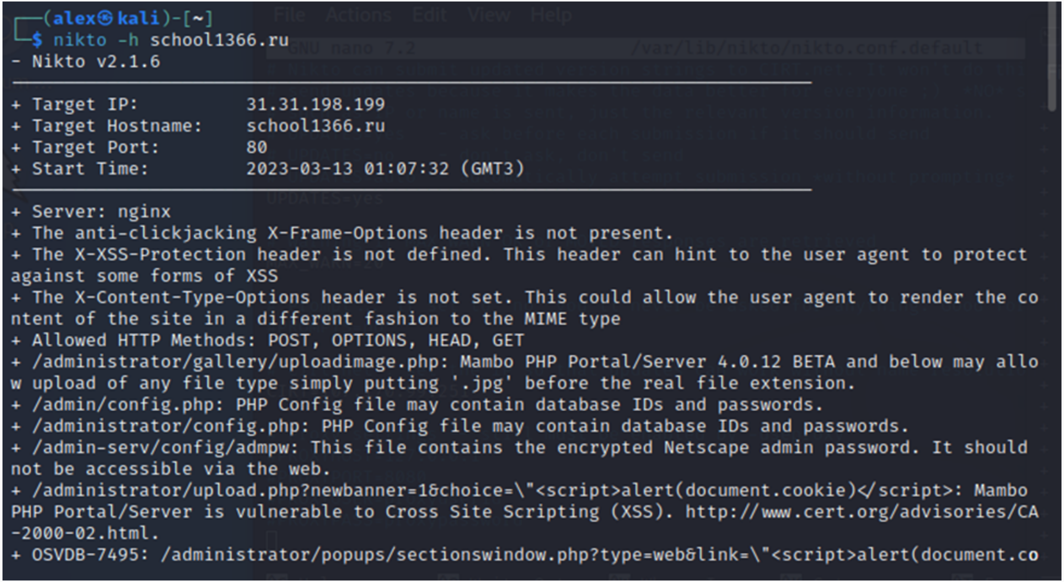
19 2024

, ,

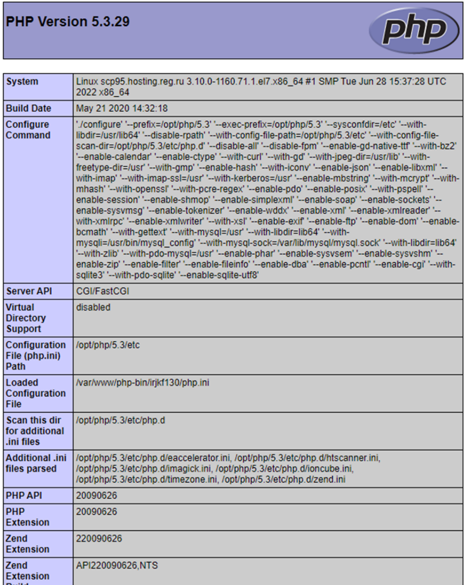
Nikto – (open source) - .
blackbox , . . , . ,
/ ( ) .
6700 .

. ,
, . Nikto (
TCP- ,) –
, , ,
.

- nikto
-



```
┌──(alex㉿kali)-[~]
└─$ nikto -h school1366.ru
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          31.31.198.199
+ Target Hostname:    school1366.ru
+ Target Port:        80
+ Start Time:         2023-03-13 01:07:32 (GMT3)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ /administrator/gallery/uploadimage.php: Mambo PHP Portal/Server 4.0.12 BETA and below may allo
w upload of any file type simply putting '.jpg' before the real file extension.
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /administrator/config.php: PHP Config file may contain database IDs and passwords.
+ /admin-serv/config/admpw: This file contains the encrypted Netscape admin password. It should
not be accessible via the web.
+ /administrator/upload.php?newbanner=1&choice=\"<script>alert(document.cookie)</script>: Mambo
PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA
-2000-02.html.
+ OSVDB-7495: /administrator/popups/sectionswindow.php?type=web&link=\"<script>alert(document.co
```



PHP Version 5.3.29

System	Linux scp95.hosting.reg.ru 3.10.0-1160.71.1.el7.x86_64 #1 SMP Tue Jun 28 15:37:28 UTC 2022 x86_64
Build Date	May 21 2020 14:32:18
Configure Command	'./configure' '--prefix=/opt/php/5.3' '--exec-prefix=/opt/php/5.3' '--sysconfdir=/etc' '--with-libdir=/usr/lib64' '--disable-rpath' '--with-config-file-path=/opt/php/5.3/etc' '--with-config-file-scan-dir=/opt/php/5.3/etc/php.d' '--disable-all' '--disable-fpm' '--enable-gd-native-ttf' '--with-bz2' '--enable-calendar' '--enable-ctype' '--with-curl' '--with-gd' '--with-jpeg-dir=/usr/lib' '--with-freetype-dir=/usr' '--with-gmp' '--enable-hash' '--with-iconv' '--enable-json' '--enable-libxml' '--with-imap' '--with-imap-ssl=/usr' '--with-kerberos=/usr' '--enable-mbstring' '--with-mcrypt' '--with-mhash' '--with-openssl' '--with-pcre-regex' '--enable-pdo' '--enable-posix' '--with-pspell' '--enable-session' '--enable-shmop' '--enable-simplexml' '--enable-soap' '--enable-sockets' '--enable-sysvmsg' '--enable-tokenizer' '--enable-wddx' '--enable-xml' '--enable-xmlreader' '--with-xmlrpc' '--enable-xmlwriter' '--with-xsl' '--enable-exif' '--enable-ftp' '--enable-dom' '--enable-bcmath' '--with-gettext' '--with-mysql=/usr' '--with-libdir=lib64' '--with-mysqli=/usr/bin/mysql_config' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-libdir=lib64' '--with-zlib' '--with-pdo-mysql=/usr' '--enable-phar' '--enable-sysvsem' '--enable-sysvshm' '--enable-zip' '--enable-filter' '--enable-fileinfo' '--enable-dba' '--enable-pcntl' '--enable-cgi' '--with-sqlite3' '--with-pdo-sqlite' '--enable-sqlite-utf8'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/php/5.3/etc
Loaded Configuration File	/var/www/php-bin/irjkf130/php.ini
Scan this dir for additional .ini files	/opt/php/5.3/etc/php.d
Additional .ini files parsed	/opt/php/5.3/etc/php.d/eaccelerator.ini, /opt/php/5.3/etc/php.d/htscanner.ini, /opt/php/5.3/etc/php.d/imagick.ini, /opt/php/5.3/etc/php.d/ioncube.ini, /opt/php/5.3/etc/php.d/timezone.ini, /opt/php/5.3/etc/php.d/zend.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS

- ,

- , , ,

, , .